УДК 004.942:004.056

к.т.н. Соколов В.В. (ORCID: 0000-0002-5779-7167)
Шаповал О.М. (ORCID: 0000-0002-4960-2235)
к.т.н. Шарадкін Д.М. (ORCID: 0000-0001-6407-8040)
(Всі - ІСЗЗІ КПІ ім. Ігоря Сікорського)

АНСАБЛЬ АЛГОРИТМІВ ВИЯВЛЕННЯ АНОМАЛІЙ В ЧАСОВИХ РЯДАХ ТА ЙОГО ВИКОРИСТАННЯ ДО ЗАДАЧ МОНІТОРИНГУ СТАНУ СИСТЕМ В РЕАЛЬНОМУ ЧАСІ

В роботі розглядається підхід до задач виявлення зміни поведінки об'єктів на основі аналізу їх моделей функціювання у вигляді часових рядів. Складність об'єктів, різноманітність форм змін поведінки, що викликані непередбаченістю як самих причин, так і їх впливу на параметри об'єкту, безперервне надходження нових даних та необхідність прийняття рішення в режимі реального часу не дозволяють обрати єдиний універсальний метод виявлення аномалій, а потребують спільного застосування їх сукупності. В роботі запропонована загальна архітектура системи виявлення аномалій в поведінці об'єкту дослідження за допомогою ансамблю алгоритмів, детально описаний кожний з її елементів. Розглянуті алгоритми, як традиційні, так і менш вживані, що можуть використовуватися в якості базових детекторів аномалій в таких системах. Досліджена низка методів узгодження рішень базових алгоритмів при узагальнені їх в остаточне рішення ансамблю, в тому числі методи, що враховують «впевненість» алгоритмів в своєму рішенні. За допомогою статистичного моделювання виконано вивчення властивостей ансамблю алгоритмів. Показано, що в складних випадках ансамбль алгоритмів дає можливість при відповідному виборі методів узагальнення показувати не гірший, а часто – кращий результат в порівнянні з базовими алгоритмами детектування аномалій, підвищити ефективності вирішення задачі як за критерієм точності прийняття рішення, так і за іншими критеріями, які використовуються в різних прикладних областях. Проведено тестування алгоритму на даних, що описують функціювання комп'ютерних мереж в стані нормального функціювання, під час атак та інших зловживань, які в ній відбуваються. Показано, що в задачах виявлення вторгнень в комп'ютерні мережі застосування ансамблевих алгоритмів може підвищити рівень безпеки, надійності та працездатності. Окреслені обмеження використання ансамблю алгоритмів та показані напрямки подальшого їх дослідження та розвитку.

Ключові слова: *виявлення аномалій, часові ряди, ансамбль алгоритмів, системи виявлення вторгнень.*

Соколов В.В, Шаповал А.Н., Шарадкин Д.М. Ансамбль алгоритмов обнаружения аномалий во временных рядах и его использование для задач мониторинга состояния систем в реальном времени*. В работе рассматривается подход к проблеме выявления изменения поведения объектов на основе анализа их моделей функционирования в виде временных рядов. Сложность объектов, разнообразие форм изменения их поведения, вызванные непредсказуемостью как причин их вызвавших, так и их влияния на параметры объекта, непрерывное поступление новых данных и необходимость принятия решения в режиме реального времени не позволяют выбрать единственный универсальный метод выявления аномалий, а требуют совместного применение их совокупности. В работе предложена общая архитектура системы обнаружения аномалий в поведении объекта исследования с помощью ансамбля алгоритмов, подробно описан каждый из ее элементов. Рассмотрены алгоритмы, как традиционные, так и менее известные, которые могут использоваться в качестве базовых детекторов аномалий в таких системах. Исследован ряд методов согласования решений базовых алгоритмов при их обобщении в окончательное решение ансамбля, в том числе методы, учитывающие «уверенность» алгоритмов в своем решении. С помощью статистического моделирования выполнено изучение свойств ансамбля алгоритмов. Показано, что в сложных случаях ансамбля алгоритмов дает возможность при соответствующем выборе методов обобщения показывать не худшие, а часто - лучшие результаты по сравнению с базовыми алгоритмами детектирования аномалий, повысить эффективности решения задачи как по критерию точности принятия решения, так и по другим критериям, которые используются в различных прикладных областях. Проведено тестирование алгоритма на данных, описывающих функционирование компьютерных сетей в состоянии нормального функционирования, во время атак и других злоупотреблений, происходящих в них. Показано, что в задачах обнаружения вторжений применение ансамблевых алгоритмов может повысить уровень безопасности, надежности и работоспособности. Описаны ограничения использования ансамбля алгоритмов, показаны направления дальнейшего их исследования и развития.*

Ключевые слова: *выявление аномалий, временные ряды, ансамбль алгоритмов, системы обнаружения вторжений.*

V.Sokolov, O.Shapoval, D.Sharadkin An Ensemble of Algorithms for Time Series Anomalies Detection and its Application for real-time systems monitoring. *The approach to changes detection in the behavior of technical objects, based on the analysis of their models in the form of time series is considered. The complexity of objects, variety of abrupt variations' behaviors influenced by the unpredictability of both reasons which caused them and their influence on the parameters of the object, the continuity of data flow, and the needs of real-time decision-making, lead*

to rejecting any single universal method for detecting anomalies and requires the joint implementation of their aggregation. A general architecture of a system for anomalies and changes detection in the behavior of an object with the utilization of the ensemble of algorithms are proposed in the paper. Each element of such system has a detailed description. Algorithms, both traditional and lesser known, that can be used as basic anomaly detectors in the system are considered. A number of methods for matching solutions of basic algorithms, including methods that respect the 'confidence' of algorithms in the solution offered, are investigated when they are generalized into the final solution of the ensemble. In complex cases, the ensemble of algorithms with an appropriate choice of generalization methods makes it possible to show not a worse yet better result than the basic anomaly detectors. It increases the efficiency of problem-solving in terms of decision accuracy, as well as other criteria used in various applications. The algorithm was tested on data describing the traffic in computer networks in normal operation, during attacks, and other abuses that occur in it. The authors show that the ensemble of algorithms implementation can increase the level of safety, reliability, and performance while addressing the problems of detecting intrusions into computer networks. The paper also covers the limitations of the ensemble of algorithms implementation, along with directions for their further research and development.

Keywords: *anomaly detection, time series, ensemble of algorithms, intrusion detection systems.*

Актуальність задачі.

У зв'язку з все більш широким використанням технічних систем реального часу виникає гостра потреба в автоматизації процесів їх моніторингу та діагностики. В загальному випадку така задача визначається як процес відстеження нормальної (типової) поведінки системи і фіксація моментів, коли поведінка істотно змінюється, а завдання діагностики - як визначення, який саме варіант нетипової (аномальної) поведінки має місце [1]. Задача моніторингу та виявлення відхилень в поведінці об'єкту дослідження виникає в багатьох сферах діяльності людини. Моніторинг технологічного обладнання вкрай важливий для підтримання працездатності промислових об'єктів. Моніторинг стану природного середовища є однією з надважливих задач забезпечення якісного життя людства. Коректний моніторинг в практичній медицині часто є умовою збереження життя пацієнту. Моніторинг криміногенного стану в регіоні здатен привернути увагу відповідних органів до соціальних проблем в ньому та знизити напругу суспільства. Моніторинг фінансового стану підприємства має виявити та вчасно запобігти небажаним відхиленням в діяльності та вчасно усунути або запобігти подальшому погіршенню стану. Таких прикладів можна навести дуже багато. Складність вирішення аналогічних задач саме в технічних об'єктах полягає в необхідності провадити збір та аналіз великого об'єму даних, здебільшого в режимі реального часу, що поступають безперервно, при підвищеній увазі до точності отриманих висновків.

Прикладом систем описаного класу є, зокрема, комп'ютерні системи та мережі, в яких процеси моніторингу реалізуються заради виявлення і запобігання інцидентів інформаційної безпеки. В таких системах в якості ознак що аналізуються використовуються інтенсивність і обсяг трафіку що циркулює в мережі, опис регламентованих і заборонених дій користувача, кількість запитів до баз даних, інформація про відмову елементів обладнання або зміни рівня його поточної завантаженості, фіксація запитів з певних IP-адресах тощо [2],[3]. Якщо в недалекому минулому з завданнями моніторингу та діагностики успішно справлялася служба системного адміністрування, то сьогодні, в зв'язку з ускладненням, масштабуванням і поширеністю систем реального часу все гостріше постає завдання автоматизації зазначених процесів.

В загальному випадку моніторинг будемо розуміти як процес спостереження за поточними значеннями параметрів об'єкту, за яким ведеться спостереження. Результат моніторингу являє сукупність виміряних значень параметрів, що були отримані на послідовних інтервалах часу. Стан об'єкту вважається нормальним якщо він виконує всі покладені на нього функції згідно заданими характеристиками та в відповідності до очікувань користувача. Відповідно аномалія – такий стан, коли поведінка об'єкту відхиляється від встановлених ознак нормальної поведінки. З математичної точки зору моніторинг та виявлення аномалій в поведінці об'єктів реального світу можна звести до

задач виявлення аномалій в поведінці моделей часових рядів, які описують параметри цих об’єктів.

Із зростанням масштабів і ускладненням сучасних системи покладатися на традиційний візуальний моніторинг і ручне виявлення відхилень в їх роботі стає все більш проблематично – як через елементарний брак персоналу, що володіє необхідними знаннями та навичками, так і через вплив, який може завдати людський фактор. Автоматизація таких задач, розробка відповідних методів, алгоритмів, підвищення їх точності, ефективності з подальшою передачею їм більшої частини рутинних обов'язків виявлення аномалій в роботі систем – нагальна задача сучасних системи он-лайн моніторингу [1].

Процедури виявлення аномалій та їх обмеження.

Аномалії, які виникають в об’єктах спостереження можуть бути найрізноманітнішими і призводили до широкого спектру змін в часових рядах значень їх параметрів. Проблеми виявлення класичних аномалій, таких як викид, контекстна та колективна аномалії (див. рис.1), описувалися та вивчалися в багатьох роботах [3], [4], [5], [6]. В них показано, що різноманітність проявів аномальних явищ вимагає застосування відповідної різноманітності методів їх виявлення, в тому числі - класифікації, кластерного, статистичного та регресійного аналізів, теорії часових рядів, методів глибокого навчання тощо. Водночас до таких видів аномалій не зводяться всі особливості, що зустрічаються при роботі з реальними технічними об’єктами та системами. Іншу групу становлять аномалії, які відображають перехід об’єкту до іншого стану, при якому часовий ряд значень його параметрів вже неможливо описати тією самою моделлю, яка використовувалася раніше. При цьому задача може ставитися або як задача виявлення самого факту вказаної зміни (задача «виявлення новизни» - novelity detection), або як задача фіксації моменту часу, коли така зміна відбулася («виявлення точки зміни моделі» - change point detection). [7], [8], [9], [10], [11]. Такі задачі вивчені та досліджені значно меншою мірою, ніж попередні. Так в роботі [12] запропоновано певні базові, типові зміни, що спостерігаються при дослідженні об’єктів в багатьох предметних областях і можуть бути використані при дослідженні відповідних алгоритмів виявлення новизни (див. рис.2).

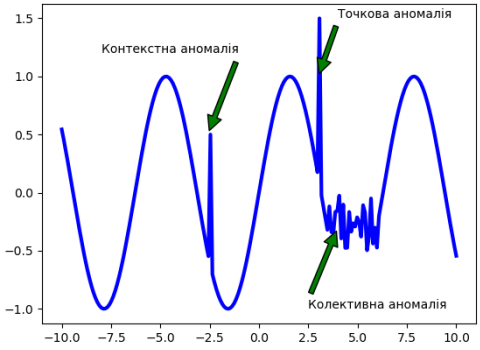

Рис. 1.Точкова, контекстна та колективна аномалії

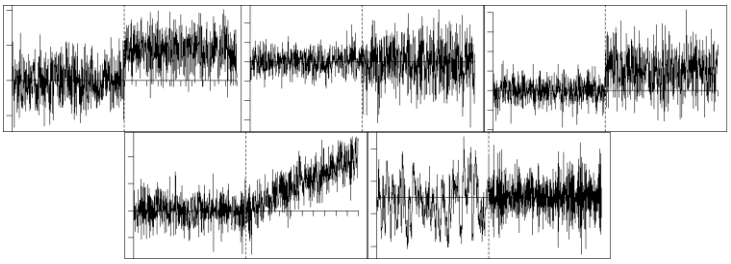

Рис. 2.Приклади зміни моделі часових рядів. Верхній ряд, зліва направо: Зміна параметру положення; Зміна параметру розкиду; Одночасна зміна параметрів положення та розкиду. Нижній ряд, зліва направо: Поява тренду; Зміна закону розподілу

Практика використання алгоритмів виявлення аномалій доводить, що кожен з відомих алгоритмів може мати високу ефективність виявлення аномальних явищ при роботі з одними наборами даних, але не працювати з іншими, характеристики яких не узгоджуються з першим набором даних. Різноманітність, складність, мінливість та необхідність роботи в реальному часі не дають можливості сподіватися на те, що буде запропонований єдиний універсальний детектор аномалій. Одна з перспективних ідей подолання вказаних труднощів полягає в застосуванні ансамблю (набору) алгоритмів, в яких результати роботи кожного базового алгоритму детектування об’єднуються заради прийняття остаточного рішення, здатного покращити показників результату відносно базових методів.

Застосовування ансамблевих методів в задачах виявлення аномалій розглянуто у [13], де увагу зосереджено в першу чергу на класі послідовних методів. В роботі [14] розглянуто ансамблевий класифікатор, пристосований для роботи з даними, що надходять в вигляді безперервного потоку та показано, що це суттєво покращило робастність методу. Методи використання ансамблів в задачах класифікації розглянуті також в роботах [15], [16]. В [17] розглянуто роботу ансамблю алгоритмів, та його використання до задачі кластеризації.

Ансамблевим методам багато уваги приділяється в сучасних задачах машинного навчання - в основному при рішенні задач класифікації. Здебільшого при цьому мова йде про аналіз даних представлених в багатовимірному просторі параметрів, де самі значення параметрів явним чином не залежать від часу. Для таких випадків використовуються методи бєггінгу, бустінгу та стекінгу. У бєггінгу кожен базовий компонент будується шляхом застосування одного і того ж базового алгоритму на випадковій проекції всього набору даних, які задані для навчання. При бустінгу базові класифікатори навчають послідовно адаптивним способом, при цьому кожний наступний класифікатор отримує результат роботи попереднього. В випадку стекінгу паралельно отримані результати базових класифікаторів об'єднують, навчаючи метамодель для отримання остаточного результату. Хоча такі методи часто показують помітне підвищення ефективності класифікації в порівнянням з методами які використовуються в якості базових, їх застосування до задач саме виявлення аномалій, особливо при аналізі процесів в часових рядах, виявляється досить обмежене [18].

Мета роботи:

Запропонувати загальну архітектуру застосунку виявлення аномалій, що використовує ансамбль базових алгоритмів детектування. Проаналізувати можливості методів узагальнення результатів базових алгоритмі та порівняти їх ефективність при використанні для різних різновидів аномалій в часових рядах.

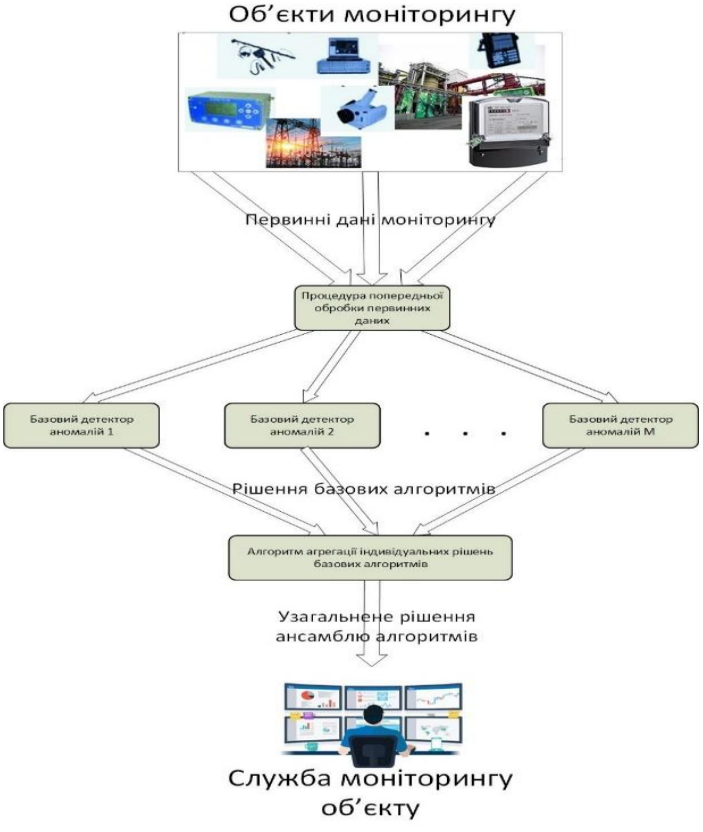

Рис. 3 Архітектура системи виявлення аномалій на основі використання ансамблю детекторів.

Архітектура системи виявлення аномалій з використанням ансамблю детекторів.

На Рис.3 відображена архітектура системи виявлення аномалій, що ґрунтується на використанні ансамблю базових детекторів аномалій. Вхідні дані надходять від відповідних сенсорів, які різняться в різних прикладних областях. Наприклад, при виявлення аномалій в роботі електромережі данні можуть надходити від вимірюючих пристроїв, що розташовані безпосередньо в лініях електроживлення. В системах метеоспостережень роль сенсорів виконують метеостанцій, що генерують дані про поточний стан погоди.

В системах виявлення аномалій в комп'ютерних мережах вхідні данні являють собою інформацію про мережевий трафік, яка надходить або від мережевого обладнання, або генеруються сніферами - спеціальними програмними застосунками захоплення трафіку. З

огляду на різноманітність аномалій, способів їх появи і прояву, має сенс розглянути якомога більше параметрів, що отримуються безпосередньо від об'єкту. Однак збільшення кількості параметрів приводить до ускладнення та уповільнення процедур їх обробки. В разі необхідності он-лайн прийняття рішення аналіз бажано проводити максимально швидко, а відтак - по можливості скоротити кількість даних, що підлягають обробці. Це протиріччя має бути якимось чином вирішено. Нажаль, загального, прийнятного для будь-якої прикладної області алгоритму скорочення не існує, і треба застосовувати фаховий аналіз. Наприклад, відомо, що в системах виявлення аномалій в комп'ютерних мережах, дані можуть отримуватися на різних рівнях мережевого протоколу. Чим вищий рівень протоколу - тим більше інформації надходить до системи, а отже точність рішення також підвищується. Однак водночас навіть сама процедура отримання даних вищих протоколів потребує поглибленого і відносно повільного парсингу, а в деяких випадках – й додаткових часових витрат на дешифрацію даних. Оскільки процедури отримання, попередньої обробки та відбору найбільш інформативних параметрів для подальшого аналізу не входить до питань, що розглядаються в роботі, будемо вважати, що дані на виході блоку а первинної обробки згенеруються у формі часового ряду, формат якого узгоджений з базовими детекторам.

Алгоритми базових детекторів аномалій.

Базові детектори аномалій представляють собою процедури, які аналізують часові ряди, що надходять на їх вхід та генерують сигнали наявності/відсутності аномалій, спираючись на відповідні статистичні процедури. Математично процедура виявлення аномалії зводиться до задачі перевірки гіпотез [1], [2], [3], [8], [9], [12], яка формально описується наступним чином:

Маємо: запис вхідного сигналу у вигляді послідовних значень часового ряду $Y = \{y_1, y_2, ...y_N\}$.

Необхідно: встановити, яка з двох визначених нижче гіпотез (H_0 або H_1) є істинною:

H_0: значення $y_1, y_2, ...y_N$ описуються єдиною моделлю поведінки $\mathfrak{M}_0$ об'єкта або системи;

H_1: існує момент часу $r : 1 < r < N$, такий що значення $y_1, y_2, ...y_r$ описуються моделлю $\mathfrak{M}_A$, а значення $y_{r+1}, y_{r+2}, ...y_N$ - моделлю $\mathfrak{M}_B$.

Однак при проведенні дослідженні виникнення змін моделі поведінки часового ряду момент коли така зміна відбувається заздалегідь невідомий. Тому процедура має дещо змінитися. Розіб'ємо наш ряд на дві рівні частини, тобто кожний з рядів бути складатися з $n = \frac{N}{2}$ значень: $Y_A = \{y_{A,1}, y_{A,2}, ...y_{A,n}\}$ та $Y_A = \{y_{A,1}, y_{A,2}, ...y_{A,n}\}$. Якщо в будь якій точці ряду Y відбулася зміна моделі, параметри рядів Y_A та Y_B будуть статистично значимо різнитися. Саме цю різницю мають підтвердити або спростувати алгоритми детектування.

Існують досить багато статистичних методів, що з різною ступеню ефективності здатні дати відповідь на вказане питання. Деякі та найбільш розповсюджені з них, реалізовані в відповідних програмних застосунках, зокрема в пакеті Scipy.stats [19], який на сьогоднішній день є стандартом де-факто як в наукових дослідженнях, так і в промисловому використанні. Нижче в наших експериментах будуть задіяні наступні методи, що реалізовані у вказаному пакеті: t-тест Ст'юдента для незалежних вибірок (t_St), ранговий тест Манна-Уитни (t_MW), тест Левене на однорідність дисперсії (t_Lv), двохвибірковий тест Колмогорова-Смірнова (t_KS). З огляду на апріорну невизначеність розподілу даних, що мають аналізуватися, вказані тести (окрім t_St) являються непараметричними. Їх опис можна знайти в [19], [20], [21].

Окрім вказаних, нижче описані тести, що були реалізовані спеціально для даного дослідження.

Тест порівняння коефіцієнту автокореляції.

Тест порівняння коефіцієнтів автокореляції (t_corr) досліджувався в [12] та показав ефективність при визначені однорідності/неоднорідності даних, зокрема в нестаціонарних часових рядах. Тест полягає в аналізі статистики

$$\omega = \frac{1}{2}\left(\left(\frac{1+r_A}{1-r_A}\right) - \ln\left(\frac{1+r_A}{1-r_A}\right)\right)\left(\frac{n^2-1}{n+1}\right) \quad (1)$$

де $r_A, r_B -$ коефіцієнти автокореляції першого порядку часових рядів Y_A та Y_B відповідно.

Позначимо $* \in \{A, B\}$, $\bar{y}'_* = \frac{1}{n-1}\sum_{i=2}^{n} y_{*i}$ $\bar{y}''_* = \frac{1}{n-1}\sum_{i=2}^{n} y_{*i-1}$. Коефіцієнт автокореляції розраховується за формулою.

$$r_* = \frac{\sum_{i=2}^{n}\left(y_{*i} - \bar{y}'_*\right)^2\left(y_{*i-1} - \bar{y}''_*\right)^2}{\sqrt{\sum_{i=2}^{n}\left(y_{*i} - \bar{y}'_*\right)^2\sum_{i=2}^{n}\left(y_{*i-1} - \bar{y}''_*\right)^2}} \quad (2)$$

Нульова та альтернативні гіпотези формулюються наступним чином:

$H_0 : \rho_A = \rho_B$

$H_{alt} : \rho_A \neq \rho_B$

де $\rho_* -$ коефіцієнти автокореляції генеральних сукупності для вибірок.

Оскільки можна вважати, що статистика ω розподілена за стандартним нормальним законом розподілу для рядів Y_A та Y_B можливо розрахувати як саме значення ω_p, так і її оцінку в вигляді p_value. Ця оцінка використовується для рішення про прийняття або відхилення гіпотези. Якщо рішення приймається на користь відкидання гіпотези H_0 це означає, що характеристики генеральних сукупностей значень рядів Y_A та Y_B різняться. Отже можна вважати, що в об'єкті відбулися внутрішні зміни, що і призвели до зміни моделей рядів. Описаний тест реалізований у вигляді процедури на мові програмування Python та використовувався як один з базових детекторів аномалій при побудові ансамблю алгоритмів.

Тест порівняння моделей регресії часового ряду.

Будь який часовий ряд або його фрагмент може бути представлений у вигляді регресійної моделі, в якій роль незалежної змінної відіграє безпосередньо час або номер відліку (тік) моменту надходження чергового значення, а роль залежної змінної - саме значення. В залежності від особливості даних регресійні рівняння обираються з обмеженого класу функцій (лінійні, квадратичні, логарифмічні, експоненційні тощо), а їх коефіцієнти визначаються виходячи з критерію мінімізації суми квадратів помилок між значеннями вхідного ряду $Y = \{y_1, y_2, ...y_N\}$ та значеннями, які генерує модель $\hat{Y} = \{\hat{y}_1, \hat{y}_2, ...\hat{y}_N\}$. Якщо вдається показати, що моделі регресії для рядів Y_A та Y_B значуще не відрізняються між собою, нульова гіпотеза про однаковість моделей - а отже і про відсутність аномалій в ряду Y - приймається. При порівнянні безпосередньо двох вказаних моделей рядів виявляється, що критерій визначення їх відмінності дуже вразливий навіть до невеликих шумів у вхідних даних. Тому для підвищення робастності пропонується використовувати дещо модифіковану процедуру, а саме будувати три моделі регресії для рядів Y_A, Y_B та $Y = \text{concatenation}(Y_A, Y_B)$. Якщо моделі статистично слабко відрізняються між собою, то гіпотезу H_0 відкинути при заданому рівні значущості α неможливо.

Прорахуємо сумарну залишкову помилку моделей, тобто

$$S_A^2=\sum_{i=n}^{n}\left(y_i-\hat{y}_i\right)^2, S_B^2=\sum_{i=n+1}^{2n}\left(y_i-\hat{y}_i\right)^2 \text{ та } S^2=\sum_{i=n}^{N}\left(y_i-\hat{y}_i\right)^2 \text{ де } N=2n.$$

При заданому рівні значущості α нульова гіпотеза відкидається, якщо F-статистика

$$F_p=\frac{\left(S_{AB}^2-S_A^2-S_B^2\right)}{\left(S_A^2+S_B^2\right)}\frac{2(n-k-1)}{(k+1)} \tag{3}$$

дає розраховане значення p_value $<\alpha$. Конкретне значення α визначається виключно семантикою задачі та визнаними стандартами в тій чи іншій предметній області. Ступені свободи розподілу F (розподілу Фішера), який використовується для обчислення p_value, приймаються рівними $(k+1)$ та $2(n-k-1)$. В формулі (3) k - кількість змінних моделі. Якщо обмежитися лінійними моделями, то $k=1$.

Описаний тест (t_regr) реалізований у вигляді процедури на мові програмування Python та також використовувався в якості одного з базових детекторів аномалій при побудові ансамблю алгоритмів.

Узгодження результатів роботи базових алгоритмів.

Остаточне рішення ансамблю про наявність або відсутність аномалії в даних може прийматися різними методами, що визначаються з огляду на конкретну прикладну задачу. Найпростіший з них – *метод консенсусу*, який приймає (або відхиляє) гіпотезу про зміну моделі ряду якщо все базові алгоритми що об'єднані в ансамбль одностайно визначили наявність (або, відповідно, відсутність) аномалії. В інших випадках відбувається відмова від прийняття рішення. Оскільки консенсус в реальних задачах досягається надзвичайно рідко, метод на практиці майже не застосовується.

Метод простої більшості.

Прийняття рішення щодо аномалії приймається в залежності від рішень, які були прийняті більшістю з базових алгоритмів. Як було показано вище, базові алгоритми приймають рішення, що отримуються з відповідних статистичних критеріїв. Ці рішення визначаються в числах, які мають різний масштаб та не можуть безпосередньо порівнюватися між собою. Тому пропонується застосувати узагальнення рішення ансамблю шляхом попереднього узгодження шкали представлення результатів базових алгоритмів.

Перший спосіб такого узгодження –- використання довірчого інтервалу. Нехай використовуються M різних базових алгоритмів, кожен з яких має виробляти рішення

$$I_m=\begin{cases}1, \text{ якщо аномалія невизначена};\\ 0, \text{ якщо аномалія визначена.}\end{cases} \tag{4}$$
$$m=1,...M$$

Для статистичних критеріїв рішення залежить від того, потрапляє розраховане значення критерію до відповідного довірчого інтервалу, чи ні. При цьому межі довірчого інтервалу явним чином залежать від обраного рівня значущості α .Таким чином, формулу (4) можна переписати як

$$I_m=\begin{cases}1, \text{ якщо } \xi_{m,p}\in\left[\xi_{m,\alpha},\xi_{m,1-\alpha}\right]\\ 0, \text{ якщо } \xi_{m,p}\notin\left[\xi_{m,\alpha},\xi_{m,1-\alpha}\right]\end{cases} \tag{5}$$

де $\xi_{m,p},\xi_{m,\alpha},\xi_{m,1-\alpha}$ – відповідно розраховане значення критерію, його верхні та нижні критичні значення.

Позначимо I_M – узагальнене рішення, що приймає ансамбль. Таке рішення приймається в залежності від того, які рішення біли прийняті більшістю з базових алгоритмів детектування аномалій, тобто:

$$I_M = \begin{cases} 1, \ якщо \sum_{m=1}^{M} I_m > \frac{M}{2}; \\ 0, \ якщо \sum_{m=1}^{M} I_m \le \frac{M}{2}. \end{cases} \quad (6)$$

Такий спосіб агрегації рішень призводить до помилки в разі, якщо більше половини базових детекторів допускаються помилки. Можливі ситуації, в яких деякі підмножини алгоритмів утворюють „коаліції", тобто результати їх роботи будуть сильно корельовані між собою. Ця корельованість є основною причиною вказаної некоректної переваги. Тому при відборі методів для множини базових детекторів рекомендується не включати в них такі, що ґрунтуються на аналогічних математичних підходах.

Методи на основі використання міри впевненості.

Описані вище способи узгодження жодним чином не враховують рівень впевненості базових детекторів в своїх рішеннях. Зрозуміло, що „впевненість" в рішенні буде різною в залежності від того, де саме – в середині довірчого інтервалу $\left[\xi_{m,\alpha}, \xi_{m,1-\alpha}\right]$ чи близько до його краю - знаходиться розраховане значення критерію $\xi_{m,p}$. В останньому разі навіть невеликі шуми в вхідних даних здатні суттєво вплинути на рішення базового алгоритму, а відтак - і на узагальнене рішення ансамблю.

В якості міри впевненості пропонується використовувати значення p_value, що його обчислює кожен з базових алгоритмів у ході своєї роботи. p_value відображає ймовірність отримати для обраної моделі розподілу значення параметрів такі самі або більші за обраховані значення статистики, за умови, що гіпотеза про відсутність аномалії в даних H_0 вірна. Таким чином рішення кожного з базових алгоритмів представляється як

$$I_m = p_{m,p} \in (0,1) \quad (7)$$

причому відкритість інтервалу означає, що абсолютну впевненість в рамках прийнятої парадигми досягти неможливо.

Запропонований підхід відкриває додаткові можливості більш гнучкого узгодження рішень базових детекторів. Перший спосіб узгодження полягає в нормованому сумуванні результатів:

$$I_M = \frac{1}{M} \sum_{m=i}^{M} I_m \quad (8)$$

Остаточне рішення приймається шліхом порівняння розрахованого значення I_M та згаданого вище параметру α, а саме гіпотеза про відсутність аномалії H_0 приймається в разі $I_M > \alpha$ та відхиляється в іншому випадку.

Наступний варіант процедури узгодження передбачає пошук найбільш впевненого в своєму рішенні базового алгоритму та прийняття рішення на його основі. Оскільки I_m трактується як впевненість алгоритму відносно гіпотези про відсутність аномалії, для визначення наявності аномалії логічно брати найменші значення $p_{m,p}$ серед тих, які були згенеровано базовими алгоритмами.

$$I_M = \min_{m=1,..M} (I_m) \quad (9)$$

Третій варіант узгодження на основі врахування впевненості полягає в використання результатів, що отримані від базових детекторів, у вигляді

$$I_m = \frac{1}{p_{m,p}} \quad (10)$$

а відповідний узагальнюючий показник впевненості формується за правилом (8).

Оцінка та порівняння алгоритмів формування узагальненого рішення.

Оцінка якості є важливим етапом аналізу алгоритмів виявлення аномалій. Для перевірки алгоритмів, їх порівняння та подальшого вдосконалення потрібно вибрати метрику, яка адекватно відображає якість моделей та способи вимірювання. Бідь яка метрика ґрунтується на кількості правильних або неправильних рішень, що алгоритм приймає при своїй роботі. Найпростіші, первинні метрики якості алгоритму вимірюються безпосередньо в процесі роботи алгоритму. До таких метрик відносяться:

TP - кількість аномалій, зафіксованих алгоритмом;

TN - кількість випадків, коли алгоритм не виявив аномалії і її в дійсності не було;

FP -кількість помилкових спрацювань, тобто фіксацій аномалії в випадку, коли в дійсності вона була відсутня (помилка першого роду);

FN - кількість аномалій, що була присутня в даних але не була зафіксована алгоритмом (помилка другого роду).

Ідеальним був би алгоритм, який міг би одночасно мінімізувати помилки і першого і другого роду, проте це теоретично неможливо [21].

Порівняння алгоритмів на основі виключно чотирьох вказаних показників не представляється доцільним в силу як їх внутрішніх протиріч, так і неможливості їх оптимізації під конкретне прикладне завдання [1], [2]. Для більш поглибленого аналізу доцільно поряд з вказаними використовувати метрики, що являються похідними від них. Це дозволяє при вирішенні конкретних задач в предметній області відібрати саме ті метрики, використання яких найбільш семантично осмислене, а отже зробити остаточний вибір на користь того чи іншого алгоритму узгодження більш обґрунтованим.

Найбільш інтуїтивно зрозумілою та очевидною похідною метрикою порівняння алгоритмів *є точність (accuracy*) – тобто відношення всіх правильно розпізнаних нормальних та аномальних ситуацій до загальної кількості тестів, які були проведені: Acc=(TP+TN)/(TP+TN+FP+FN). Нажаль, ця метрика тим менше відповідає потребам дослідника, чим менш збалансована кількість нормальних та аномальних випадків, які присутні в даних. Якщо в одних предметних областях така розбалансованість зустрічається рідко, то в інших - це звичайне явище.

Точність (precision), показує, яку долю випадків, що були позначені як аномальні, такими являються і в дійсності: Pr=(TP)/(TP+FP). *Повнота (recall*) показує, який процент серед всіх аномалій, що в дійсності містяться в даних був виявлений: Re=(TP)/(TP+FN). На відміну від долі правильних відповідей Acc, точність та повнота не залежать від співвідношення кількості об’єктів класів і тому лишаються коректними навіть в умовах незбалансованих вибірок. *Рівень помилкових спрацювань (false positive rate)* - кількість виданих сигналів про наявність аномалії в разі, коли такої аномалії в дійсності не було: Fpp=FP/(TN+FP).

Загалом не існує алгоритму, який би однаково ефективно працював на різних даних, та демонстрував би однаково високі показники по всім зазначеним метрикам. Часто в реальній практиці необхідно знайти певний прийнятний для даної задачі баланс між точністю та повнотою. Тоді визначивши стратегію та ресурси для досягнення значення одного з цих показників, можливо визначити відповідні допустимі пороги значень іншого.

Експериментальне дослідження запропонованого рішення та його аналіз.

Проведене дослідження ставило за мету по-перше виявити, чи можна вважати, що використання ансамблю алгоритмів здатне підвищити якість виявлення аномалій порівняно з окремим використанням кожного базового алгоритму детектування, а по-друге виявити, в яких випадках який з способів узгодження результатів базових детекторів дає найкращий результат.

План дослідження.

Як було описано вище, в різних задачах можливо виникнення аномалій різноманітної природи. Тому дослідження передбачало застосування побудованих ансамблевих алгоритмів виявлення аномалій до набору тестових даних. Кожний з різновидів аномалій (Рис.2) генерувався відповідною функцією-генератором 1000 раз, причому для збереження чистоти

експерименту, кожна така генерація включала як зразок даних без аномалій, так і зразок даних з аномалією.

В усіх експериментах довжина рядів Y_A та Y_B дорівнювала 100. Оскільки зрозуміло, що будь яка аномалія, що почалася на одному з перших відліків часового ряду об'єктивно має вищий шанс бути зафіксованою, аніж аномалія, що виникла на останніх його відліках, сам момент початку виникнення аномалій теж визначався за допомогою генератора випадкових чисел.

Оскільки в реальних задачах нам невідомо, які саме аномалії виникнуть, результати всіх експериментів узагальнювалися. Для цього результати роботи кожного з базових алгоритмів фіксувалися окремо, а потім передавалися на обробку алгоритмам узгодження. Отримані таким чином результати наведені в Таблиці 1.

Аналіз результатів.

Таблиці 1. виділено по два найкращих показники по кожній з метрик. (Для параметрів TN, TP, Prec, Rec - чим більше тим краще, для параметрів FP, FN,FPP - чим менше, тим краще). Також для метрик безпосереднього вимірювання показано, на скільки процентів різняться результати кожного з алгоритмів узгодження в порівняні з найкращим для даної метрики показником серед базових алгоритмів.

Аналіз таблиці показує, що ансамбль детекторів в більшості випадків здатен покращити показники розпізнавання в порівнянні з результатами застосування кожного з базових алгоритмів окремо.

Так, якщо з семантики предметної області випливає, що переважне значення мають питання саме виявлення (не пропуск) аномалій, то найкращим вибором може бути алгоритми rev_min та c_sum, побудовані за формулами (9) та (10) відповідно.

Якщо головна проблема полягає в необхідності зменшення кількості хибних спрацювань, то перевагу слід віддати алгоритмам max та wgh, що побудовані за формулами (6) та (8). При пошуку деяких компромісних варіантів можна спиратись на результати похідних метрик – Prec, Recall, та Fpp.

Таблиця 1.

Результати роботи базових детекторів та алгоритмів узгодження їх рішень

Test	TN		FP		FN		TP		Prec	Recall	FPP
t_St	4729		271		2172		2828		0.913	0.566	0.054
t_MW	4475		525		2251		2749		0.840	**0.550**	0.105
t_Lv	4772		228		1151		3849		0.944	0.770	0.046
t_KS	**4801**		199		1846		3154		0.941	0.631	0.040
t_corr	4728		272		1162		3838		0.934	0.768	0.054
t_regr	4749		251		1685		3315		0.930	0.663	0.050
max	4755	0.990	**195**	0.980	1304	1.133	3696	0.960	**0.950**	0.739	**0.039**
wgh	**4873**	1.015	**127**	0.638	2351	2.043	2649	0.688	**0.954**	**0.530**	**0.025**
rev_min	4100	0.854	900	4.523	**812**	0.705	**4188**	1.088	0.823	0.838	0.180
c_sum	4677	0.974	323	1.623	**1096**	0.952	**3904**	1.014	0.924	0.781	0.065

В якості реальних даних, на яких досліджувалися запропоновані методи, використовувалися дані з відкритого набору Intrusion Detection Evaluation Dataset (CIC-IDS2017), що вільно доступний в дослідницьких цілях [22].

Набор містить як доброякісні дані, так і зразки трафіку з найсучаснішими найбільш поширеними атаками, такими як Web based, Brute force, DoS, DDoS, Infiltration, Heart-bleed, Bot and Scan. На відміну від багатьох інших наборів, даний набір в тому числі надає «сирі»

дані в форматі pcap, що дає можливість використати параметри трафіку, найбільш придатні саме для задач он-лайн виявлення аномалій в комп'ютерній мережі.

По результатам проведеного дослідження виявлено, що ансамблеві алгоритми, що розглянуті в роботі, дозволяють і на реальних даних отримати підвищення ефективності роботи по відношенню до базових алгоритмів. Так для атак типу DoS точність ансамблевих алгоритмів перевищувала точність найкращого з базових алгоритмів на 3-6 %, для атак Infiltration – на 2-7 % .

На якість виявлення атак в трафіку значно впливає базовий стан мережі, тобто стан, що приймався за нормальний. Показники підвищення ефективності ансамблю по відношенню до базових детекторів при одній інтенсивності зловмисного втручання але різних базових активностях можуть коливатися від 0.1 до 10-12 %. Дослідження в даному напрямі продовжуються.

Висновки та подальший напрям дослідження.

В роботі досліджувалась можливість використання ансамблевих алгоритмів для покращення ефективності систем виявлення аномалій в часових рядах. Для підвищення селективної спроможності до множини базових алгоритмів детектування аномалій були включені як широковідомі статистичні методи, так і менш вживані методи на основі аналізу коефіцієнту автокореляції та моделі регресії рядів.

Проведені експерименти з застосуванням набору синтезованих тестових аномалій які характерні для різних прикладних областей показали, що за допомогою запропонованих алгоритмів узагальнення вдається підвищити значення метрик якості в порівнянні з кожним з базових алгоритмів.

Для деяких з методів узагальнення покращення спостерігалося одночасно по трьом та п'ятьом (з семи) метрикам одночасно.

Експеримент на наборі даних, що описує реальний мережевий трафік також підтвердив підвищення якості розпізнавання. В подальшому розвитку робіт планується вивчити питання більш точного обґрунтування складу ансамблю базових алгоритмів детектування, а також дослідити вплив вибору конкретної підмножини параметрів, що отримуються від одного об'єкту на точність отриманих результатів.

ЛІТЕРАТУРА

1.Pascual D.G. Artificial Intelligence Tools: Decision Support Systems in Condition Monitoring and Diagnosis. CRC Press. 2015 – 549 p.

2. Collins M. Network Security Through Data Analysis. Sebastopol, CA, USA: O'Reilly Media Inc., 2014.– 325p.

3. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии) М.: Горячая линия—Телеком, 2013.– 220с.

4. Xu X., Liu H., Yao M. Recent Progress of Anomaly Detection. In Hindawi Complexity. Vol.2019, Article ID 2686378, 11p. doi:10.1155/2019/2686378.

5. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey. In ACM Comput. Surv., 41(3):2009.p.1-58. doi:10:1145/1541880:1541882.

6. Mehrotra K.G., Mohan C.K., Huang H.M. Anomaly Detection. Principles and Algorithms. Springer International Publishing AG 2017.-229 p. doi:10.1007/978-3-319-67526-8.

7. Chen J., Gupta A.K. Parametric Statistical Change Point Analysis: With Applications to Genetics, Medicine, and Finance Birkhäuser Basel Year: 2012.– 282p.

8. Никифоров И.В. Последовательное обнаружение изменения свойств временных рядов. М:,"Наука",1983.– 200с.

9. Aminikhanghahi S., Cook D.J. A Survey of Methods for Time Series Change Point Detection. In Knowl Inf Syst. 2017 May ; 51(2): 339 – 367p.

10. Fearnhead P., Rigaill G. Changepoint detection in the presence of outliers. In Journal of the American Statistical Association, 114(525):169-183, 2019. doi:10.1080/01621459.2017.1385466.

11. Truong C., Oudre L., Vayatis N.Selective review of offline change point detection methods. In Signal Processing, 167:107299, 2020.

12. Шарадкін Д.М.,Використання критерію виявлення змін поведінки об'єкта на основі аналізу коефіцієнта автокореляції в задачах забезпечення інформаційної безпеки. Information Technology and Security. January-June 2017. Vol. 5. Iss.1(8). p.42 – 54.

13. Zhao Z., Ensemble Methods for Anomaly Detection (2017). Dissertations – ALL. 817.
https://surface.syr.edu/etd/817

14. Farid D.M., Zhang L., Hossain A., Rahman C.M., Strachan R., Sexton G., Dahal K. An adaptive ensemble classifier for mining concept drifting data streams. Expert Syst Appl 40(15), 2013: p.5895–5906.doi:10.1016/j.eswa.2013.05.001.

15. Kuncheva L. I. Combining pattern classifiers : methods and algorithms. John Wiley & Sons, Inc., Hoboken, New Jersey. 2014.– 382p.

16. Rokach L. Ensemble-based classifiers. In Artif Intell Rev (2010) 33:p.1-39.doi:10.1007/s10462-009-91247.

17. Rayana S., Akoglu L. Less is more: Building selective anomaly ensembles. ACM Transactions on Knowledge Discovery from Data (TKDD) 10, 4 (2016), p.1 – 33. doi:10.1145/2890508.

18. Molin-Ribeiro M.H.D., Santos L. Ensemble approach based on bagging, boosting and stacking for short-term prediction in agribusiness time series. Applied Soft Computing Vol. 86, January 2020, 105837. doi:10.1016/j.asoc.2019.105837.

19. SciPy library. URL: https://scipy.org/scipylib/index.html (дата звернення: 23.01.2021).

20. Кобзарь А.И., Прикладная математическая статистика. Для инженеров и научных работников, Москва,РФ: ФИЗМАТЛИТ, 2006.– 861с.

21. Лемешко Б.Ю. Критерии проверки гипотез об однородности. Руководство по применению. Новосибирск, 2016. – 207с.

22.Intrusion Detection Evaluation Dataset (CIC-IDS2017).
UR L: https://www.unb.ca/cic/datasets/ids-2017.html (дата звернення: 23.01.2021).